ТЕХНИЧЕСКИЙ КОДЕКС УСТАНОВИВШЕЙСЯ ПРАКТИКИ

ТКП 287-2010 (07040)

Банковские технологии
Внутренний контроль и аудит информационных систем

Банкаўскія тэхналогіі
Унутраны кантроль і аудыт інфармацыйных сістэм

Издание официальное

Национальный банк Республики Беларусь
Минск

УДК МКС 35.240.40 КП 05

Ключевые слова: банковские технологии, внутренний контроль, внутренний аудит, аудитор, информационные системы.

Предисловие

1 РАЗРАБОТАН Открытым акционерным обществом «Центр банковских технологий»
ВНЕСЕН Национальным банком Республики Беларусь

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Правления Национального банка Республики Беларусь от 10.12.2010 № 540

3 ВВЕДЕН ВПЕРВЫЕ

Издан на русском языке

Содержание

ТЕХНИЧЕСКИЙ КОДЕКС УСТАНОВИВШЕЙСЯ ПРАКТИКИ

Банковские технологии
Внутренний контроль и аудит информационных систем

Банкаўскія тэхналогіі
Унутраны кантроль і аудыт інфармацыйных сістэм

Banking technologies
Internal control and auditing of IMS (information systems)

Дата введения 2011-03-01

1 Область применения

Настоящий технический кодекс установившейся практики (далее – технический кодекс) устанавливает общие требования к процедурам внутреннего контроля и внутреннего аудита информационных систем банков.

Использование банками настоящего технического кодекса носит добровольный характер, если только в отношении отдельных положений обязательность их применения не установлена законодательством Республики Беларусь, иными нормативными правовыми актами, в том числе нормативными правовыми актами Национального банка Республики Беларусь.

При применении технического кодекса банками обязательна ссылка на него и (или) прямого использования устанавливаемых в нем положений в локальных нормативных правовых актах банков, а также в договорах. При этом требования технического кодекса, содержащие положения долженствования, применяются на обязательной основе, а рекомендации применяются по решению банка.

Технический кодекс определяет общие требования к процедурам внутреннего контроля следующих групп процессов в отношении информационных систем:

– планирование и организация;
– приобретение и внедрение;
– эксплуатация и сопровождение;
– мониторинг и оценка.

Предполагается, что выполнение положений технического кодекса поручается компетентным лицам с соответствующей квалификацией.

Издание официальное

2 Нормативные ссылки

В техническом кодексе использованы ссылки на следующие технические нормативные правовые акты в области технического нормирования и стандартизации:

СТБ П ISO/IEC 27001-2008 Информационные технологии. Технологии безопасности. Системы управления защитой информации. Требования

СТБ П 34.101.41-2009 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения

СТБ П 34.101.42-2009 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Аудит информационной безопасности

3 Термины и определения

В техническом кодексе применяют следующие термины с соответствующими определениями:

3.1 владелец данных (информации): Субъект, реализующий права владения, пользования и распоряжения данными (информацией) в соответствии с законодательством Республики Беларусь и локальными нормативными правовыми актами банка.

3.2 владелец процесса: Субъект, ответственный за выполнение процесса в соответствии с законодательством Республики Беларусь и локальными нормативными правовыми актами банка.

3.3 внутренний аудит информационной системы; внутренний аудит ИС: Системный процесс получения объективных данных о состоянии информационной системы, а также внешних и внутренних факторах, влияющих на функционирование информационной системы, включая систему внутреннего контроля ИС, с целью оценки соответствия информационной системы установленным требованиям и целям (критериям аудита).

3.4 информационная система; ИС: Совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств.

3.5 инцидент: Любое событие, не являющееся штатным элементом сервиса ИС, которое вызывает сбой или снижение качества ее функционирования.

3.6 мера: Стандарт, применяемый для оценки эффективности в связи с ожидаемыми результатами.

3.7 персонал ИС: сотрудники банка, выполняющие функции необходимые для обеспечения функционирования ИС банка.

3.8 пользователь информационной системы и (или) информационной сети; пользователь ИС: работник банка, получивший доступ к ИС и (или) информационной сети и пользующийся ими при исполнении должностных обязанностей.

3.9 проблема: Неизвестная причина, лежащая в основе одного или многих инцидентов в ИС.

3.10 процедура: Документированный порядок, включающий в себя последовательность действий, описывающих достижение результата. Процедуры определяются как часть процессов.

4 Общие положения

4.1 Система внутреннего контроля ИС входит в состав общей системы внутреннего контроля и общей системы управления информационными технологиями (далее – ИТ) банка и должна состоять из совокупности согласованных правил, инструкций, процедур и средств внутреннего контроля ИС.

4.2 Правилами внутреннего контроля ИС регламентируется процесс осуществления внутреннего контроля ИС и его структура.

4.3 В дополнение к правилам внутреннего контроля ИС должны использоваться документированные процедуры по выполнению проверок оборудования, программного обеспечения, процессов, операций и персонала ИС.

4.4 Процедуры внутреннего контроля ИС должны подвергаться плановым проверкам и пересматриваться внепланово в случаях изменений в техническом или программном оснащении ИС, изменении технологических процессов, изменении организационной структуры.

4.5 Программно-технические средства внутреннего контроля ИС рекомендуется интегрировать в ИС для реализации внутренних контролей ИС в автоматизированном или автоматическом режиме, включая контроль ввода и обработки данных, доступа к ИС, а также контроль состояния процессов в ИС.

4.6 Функционирование системы внутреннего контроля ИС должно быть обеспечено соответствующими ресурсами: персонал, оборудование и программное обеспечение.

4.7 ИС подлежат регулярному внутреннему аудиту в соответствии с планами проведения внутреннего аудита ИС.

4.8 Помимо плановых аудиторских проверок могут проводиться внеплановые проверки ИС. Внеплановые проверки ИС как правило, выполняются в случаях существенных изменений в техническом или программном оснащении ИС, технологических процессов, организационной структуры.

4.9 Персонал, ответственный за проведение внутреннего аудита ИС, кроме обладания необходимой квалификацией должен быть независим от тех, кто непосредственно отвечает за функционирование ИС и проверяемые виды деятельности.

5 Общие требования к процедурам внутреннего контроля информационной системы банка

Все ИТ-процессы в отношении ИС должны контролироваться. Базовая модель контроля показана на рисунке 1.

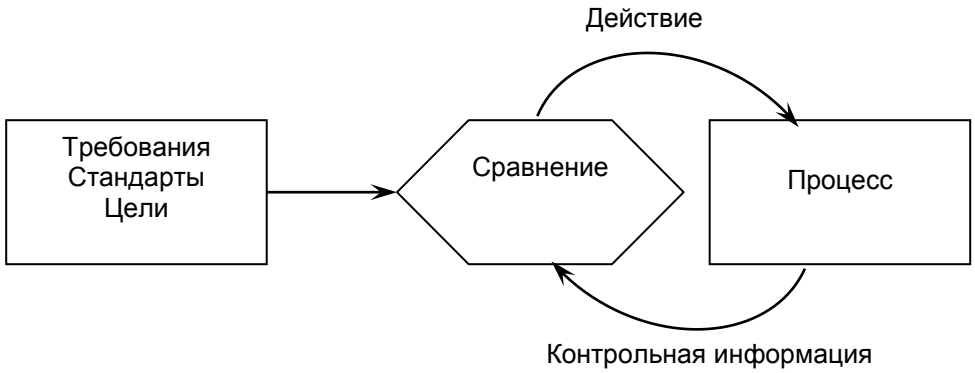

Рисунок 1

Общие требования к процедурам внутреннего контроля ИТ-процессов:

– определить измеряемые, исполнимые, реалистичные, ориентированные на результат цели и задачи для эффективного выполнения каждого ИТ-процесса. Следует убедиться, что цели и задачи процесса связаны с бизнес-целями и обеспечены соответствующими шкалами оценки;

– определить владельца для каждого ИТ-процесса, четко сформулировать его роли и сферы ответственности;

– разработать и реализовать каждый ключевой ИТ-процесс таким образом, чтобы он был повторяемым и постоянно приносил ожидаемые результаты. Создать логичную, но гибкую и масштабируемую последовательность действий, которая приведет к желаемым результатам и будет достаточно гибкой для нестандартных ситуаций и экстренных случаев. Использовать последовательные процессы во всех случаях, когда это возможно, и видоизменять их только когда это неизбежно;

– определить ключевые действия и конечные результаты процесса. Назначить и донести однозначное понимание ролей и ответственностей для эффективного и результативного исполнения и документирования ключевых действий, а также для отчетности по конечным результатам процесса;

– определить и донести до всех заинтересованных сторон, процедуры ИТ-процессов. Процедуры должны документироваться, пересматриваться, поддерживаться утверждаться, храниться и использоваться для обучения. Убедиться, что процедуры доступны, правильны, понятны и актуальны;

– определить набор показателей, которые позволят оценить результаты и эффективность ИТ-процесса. Поставить конкретные задачи, которые соответствуют целям процесса и выявить показатели, которые отражают достижение этих целей. Описать, как должен происходить сбор данных. Сравнить текущие показатели с планируемыми и при необходимости действовать с учетом возможных отклонений. Сопоставить показатели, цели и методы в рамках единого подхода к оценке эффективности ИТ-процессов.

5.1 Требования к процедурам внутреннего контроля в процессах планирования и организации информационной системы банка

5.1.1 В процессах планирования и организации ИС необходимо осуществлять контроль за:

– разработкой планов создания и развития ИС;

– определением информационной архитектуры ИС;

– определением направления технологического развития ИС;

– определением ИТ-процессов, организационной структуры и взаимосвязей ИС;

– управлением бюджетом создания, развития и эксплуатации ИС;
– разработкой методологии внутреннего контроля для ИС;
– управлением персоналом ИС;
– управлением качеством ИТ-процессов;
– оценкой и управлением ИТ-рисками, как категорией операционного риска;
– управлением ИТ-проектами.

5.1.1.1 В процессе разработки планов создания и развития ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– обоснования планов создания и развития ИС;
– выполнения оценки рисков не реализации поставленных целей и задач;
– адекватности используемых методик обоснования необходимости создания или развития ИС и правильность сделанных на их основе выводов;
– обоснования решений по созданию и развитию ИС;
– структуры планов, в частности наличие в тактических планах задач, обеспечивающих контроль за отклонениями от выполнения, включая изменения по стоимости, графику или функциональности, которые могут повлиять на ожидаемые результаты;
– качества используемой внутренней и внешней информации;
– соблюдения действующего законодательства и локальных нормативных правовых актов.

5.1.1.2 В процессе определения информационной архитектуры ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– создания и поддержки модели данных ИС в соответствии с заранее определенной методологией построения информационной архитектуры ИС и планами развития ИС;
– обеспечения точности и корректности информационной архитектуры и модели данных;
– ведения справочника данных ИС, включающего в себя правила представления данных;
– назначения владельцев данных (информации);
– классификации информации в соответствии с заранее согласованной классификационной схемой, основанной на критичности и значимости данных (например, общедоступные, конфиденциальные и др.);
– обеспечения целостности, непротиворечивости и совместимости всех данных, хранящихся в электронной форме, таких как базы, хранилища и архивы данных.

5.1.1.3 В процессе определения направления технологического развития ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– планирования технологической инфраструктуры ИС;
– выполнения анализа перспективных направлений, технологий и тенденций в области нормативного регулирования;
– разработки и развития технологических стандартов и инструкций;
– разработки планов развития технологической инфраструктуры ИС;
– информирования заинтересованных сторон и их участие в планировании развития технологической инфраструктуры ИС;
– оценки ИТ-рисков при разработке новых возможностей ИС.

5.1.1.4 В процессе определения ИТ-процессов, организационной структуры и взаимосвязей ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– наличия и разработки методологии ИТ-процессов;
– создания организационной структуры ИС;
– потребности и стратегии в области аутсорсинга, в том числе соотношения между персоналом ИС банка и сторонними специалистами;
– определения должностных обязанностей и полномочий персонала ИС и пользователей ИС;
– назначения ответственного персонала ИС по вопросам обеспечения качества и их обеспечения соответствующими средствами контроля и информирования;
– назначения ответственного персонала ИС за управление ИТ-рисками, информационной и физической безопасностью;
– определения ключевого персонала ИС и минимизации зависимости от конкретных специалистов в исполнении критических функций;
– оптимальности внутренних и внешних взаимосвязей ИС.

5.1.1.5 В процессе управления бюджетом создания, развития и эксплуатации ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– формирования бюджета;

– управления затратами.

5.1.1.6 В процессе разработки методологии внутреннего контроля для ИС процедуры должны содержать меры, обеспечивающие контроль:

– определения элементов среды контроля для ИС;

– определения общих подходов к ИТ-рискам и методам их контроля;

– документирования методологии и процедур контроля для ИС.

5.1.1.7 В процессе управления персоналом процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– найма и обучения персонала ИС;

– компетентности персонала ИС;

– распределения обязанностей;

– оптимальности численности персонала;

– эффективности работы персонала ИС;

– зависимости от отдельных ключевых трудовых ресурсов;

– выполнения надлежащих мер при переходе персонала ИС на другую работу или увольнении (передача знаний, перераспределение ответственностей и ликвидация прав доступа).

5.1.1.8 В процессе управления качеством ИТ-процессов процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– создания и поддержки системы управления качеством ИТ-процессов;

– определения стандартов и инструкций по управлению качеством, включая стандарты в области разработки и приобретения компонентов ИС;

– определения системы измерений уровня качества ИТ-процессов.

5.1.1.9 В процессе оценки и управления ИТ-рисками процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– определения методологии управления ИТ-рисками и ее интеграции в методологию управления операционным риском;

– идентификации ИТ-рисков;

– оценки вероятности и последствий реализации идентифицированных ИТ-рисков;

– разработки планов обработки ИТ-рисков.

5.1.1.10 В процессе управления ИТ-проектами процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– определения методологии управления ИТ-проектами;

– планирования ИТ-проектов;

– определения ресурсов ИТ-проектов;

– определения рисков ИТ-проектов;

– обеспечения качества ИТ-проектов;

– определения системы контроля за внесением изменений в ИТ-проекты;

– эффективности ИТ-проектов по охвату, срокам реализации, качеству, затратам и рискам.

5.2 Требования к процедурам внутреннего контроля в процессах приобретения и внедрения информационной системы в банке

5.2.1 В процессах приобретения и внедрения ИС необходимо осуществлять контроль за:

– выбором решений по автоматизации;

– приобретением и организацией поддержки программных приложений;

– приобретением и организацией обслуживания технологической инфраструктуры;

– обеспечением обучения пользователей и персонала ИС;

– управлением договорными отношениями с поставщиками ИС;

– организацией внесения изменений в ИС;

– внедрением и принятием решений и изменений в ИС.

5.2.1.1 В процессе выбора решений по автоматизации процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– определения и обоснования требований к функциональности ИС;

– анализа рисков, связанных с реализацией требований к функциональности ИС;

– разработки основного и альтернативного планов действий по реализации требований.

5.2.1.2 В процессе приобретения и организации поддержки программных приложений ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– преобразования требований к ИС в спецификации на приобретение программного обеспечения;

– определения дизайна приложений и технических требований к программному обеспечению;

– внедрения контрольных функций ИС в программные приложения;

– выполнения требований к безопасности и доступности программных приложений в соответствии с выявленными рисками и принятой в банке классификацией данных, информационной архитектурой, архитектурой информационной безопасности и уровнем принятых рисков;

– конфигурирования и внедрения приобретенного программного обеспечения;

– разработки программных приложений;

– обеспечения качества программных приложений;

– управления требованиями к программным приложениям;

– разработки стратегии и плана поддержки программных приложений.

5.2.1.3 В процессе приобретения и организации обслуживания технологической инфраструктуры ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– планирования приобретения технологической инфраструктуры;

– внедрения критериев контроля и безопасности в процессе конфигурирования, интеграции и обслуживания аппаратного обеспечения и системного программного обеспечения;

– создания среды тестирования компонентов технологической инфраструктуры ИС;

– разработки стратегии и плана обслуживания технологической инфраструктуры ИС.

5.2.1.4 В процессе обеспечения обучения пользователей ИС и персонала ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– приобретения и разработки документации для пользователей и персонала ИС;

– планирования и организации обучения пользователей ИС эффективному и оптимальному использованию ИС для поддержки бизнес-процессов;

– планирования и организации обучения персонала ИС эффективному и оптимальному обслуживанию ИС и связанной с ней инфраструктуры.

5.2.1.5 В процессе управления договорными отношениями с поставщиками ИС или ее компонентов процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– разработки и применения процедур осуществления поставок и стратегии в области закупок компонентов инфраструктуры ИС, в том числе аппаратного и программного обеспечения, а также услуг;

– управления договорами с поставщиками;

– выбора поставщиков.

5.2.1.6 В процессе организации внесения изменений в ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– организации применения формализованных процедур в области управления изменениями для стандартизованной обработки всех запросов на изменения;

– организации проведения оценки всех запросов на изменения;

– установления процесса определения, заявления, тестирования, документирования, оценки и авторизации аварийных изменений;

– установления системы мониторинга и отчетности по статусу изменений;

– организации процесса обновления документации ИС при реализации изменений.

5.2.1.7 В процессе внедрения и приемки решений и изменений в ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– проведения обучения пользователей и персонала ИС в соответствии с определенными планами;

– планирования и проведения тестирования изменений;

– ввода изменений в промышленную эксплуатацию;

– анализа результатов ввода изменений в промышленную эксплуатацию.

5.3 Требования к процедурам внутреннего контроля в процессах эксплуатации и сопровождения информационной системы банка

5.3.1 В процессах эксплуатации и сопровождения ИС необходимо осуществлять контроль за:

– управлением уровнем обслуживания ИС, в том числе сторонними организациями;

– управлением производительностью и мощностями ресурсов ИС;

– обеспечением непрерывности функционирования ИС;

– обеспечением информационной безопасности ИС;

– обучением пользователей и персонала ИС;
– управлением инцидентами;
– управлением конфигурацией ИС;
– управлением проблемами;
– управлением данными в ИС;
– обеспечением физической безопасности и защиты ИС от воздействия окружающей среды;
– управлением операциями по эксплуатации ИС.

5.3.1.1 В процессе управления уровнем обслуживания ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– разработки методологии управления уровнем обслуживания ИС, включающей требования к услугам сторонних организаций, определение ответственности внутренних и внешних поставщиков и потребителей ИТ-услуг;
– определения ИТ-услуг;
– формирования и заключения соглашений об уровне обслуживания для всех критичных ИТ-услуг;
– управления рисками, связанными с аутсорсингом ИТ;
– выполнения соглашений об уровне обслуживания.

5.3.1.2 В процессе управления производительностью и мощностями ресурсов ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– текущей производительности и мощности ИТ-ресурсов;
– прогнозирования производительности и мощностей ИТ-ресурсов;
– доступности ИТ-ресурсов;
– осуществления мониторинга производительности и мощностей ИТ-ресурсов.

5.3.1.3 В процессе обеспечения непрерывности функционирования ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– разработки документации по обеспечению непрерывности функционирования ИС;
– планирования обеспечения непрерывной работы и восстановления ИС;
– тестирования планов обеспечения непрерывной работы и восстановления ИС;
– актуализации планов обеспечения непрерывной работы и восстановления ИС;
– регулярного обучения персонала ИС и заинтересованных сторон по выполнению соответствующих процедур по планам обеспечения непрерывной работы и восстановления ИС;
– обеспечения доступности и ознакомления с планами обеспечения непрерывной работы и восстановления ИС заинтересованных сторон.

5.3.1.4 В процессе обеспечения информационной безопасности ИС процедуры внутреннего контроля должны соответствовать требованиям СТБ П ISO/IEC 27001-2008, СТБ П 34.101.41-2009, СТБ П 34.101.42-2009.

5.3.1.5 В процессе обучения пользователей и персонала ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– определения потребностей в обучении пользователей ИС и персонала ИС;
– планирования обучения;
– проведения обучения;
– актуальности, качества и эффективности обучения.

5.3.1.6 В процессе управления инцидентами процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– регистрации обращений пользователей;
– разрешения инцидентов и фиксации механизмов их решения;
– учета неразрешенных инцидентов;
– эффективности разрешения инцидентов, выявления тенденций или повторяющихся проблем.

5.3.1.7 В процессе управления конфигурацией ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– учета и хранения всех конфигурационных данных и изменений в них;
– целостности и наличия отклонений в конфигурации ИС;
– программного и аппаратного обеспечения ИС на предмет соответствия установленным в банке требованиям;
– приобретения и учета лицензий.

5.3.1.8 В процессе управления проблемами процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– выявления и классификация проблем;

– учета, отслеживания, разрешения и устранения проблем.

5.3.1.9 В процессе управления данными в ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– обработки данных в соответствии с установленными требованиями;

– записи, хранения и архивирования данных;

– использования и вывода из эксплуатации носителей данных;

– резервного хранения и восстановления данных;

– выполнения требований по безопасности в отношении записи, обработки, хранения и вывода данных.

5.3.1.10 В процессе обеспечения физической безопасности и защиты ИС от воздействия окружающей среды процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– определения и внедрения показателей физической безопасности помещений для размещения оборудования и персонала ИС;

– предоставления, ограничения и прекращения доступа в помещения, здания и территории размещения инфраструктуры ИС;

– защиты оборудования ИС от факторов внешней среды;

– управления оборудованием ИС и выполнения процедур по техническому обслуживанию в соответствии с инструкциями, техническими требованиями, спецификациями поставщиков, требованиями по технике безопасности и охране здоровья.

5.3.1.11 В процессе управления операциями по эксплуатации ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– определения, реализации и поддержки процедур и инструкций для операций по эксплуатации ИС;

– составления графика работ, процессов и задач по эксплуатации ИС;

– мониторинга инфраструктуры ИС и относящихся к ней событий, протоколирования операций и другой деятельности, связанной с поддержкой операций;

– определения и реализации на практике процедур, обеспечивающих оперативную поддержку инфраструктуры ИС, в том числе планового обслуживания оборудования.

5.4 Требования к процедурам внутреннего контроля в процессах мониторинга и оценки информационной системы банка

5.4.1 В процессах мониторинга и оценки ИС необходимо осуществлять контроль за:

– организацией мониторинга и оценкой эффективности ИС;

– мониторингом и оценкой системы внутреннего контроля ИС;

– обеспечением соответствия ИС внешним требованиям;

– обеспечением корпоративного управления ИС.

5.4.1.1 В процессе организации мониторинга и оценки эффективности ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– формирования и внедрения методик мониторинга и оценки эффективности ИС;

– определения подлежащих мониторингу основных показателей и сбора данных, приемлемых для оценки эффективности ИС;

– формирования отчетности по результатам мониторинга;

– реализации корректирующих действий, основанных на результатах мониторинга и оценки эффективности.

5.4.1.2 В процессе мониторинга и оценки внутреннего контроля ИС процедуры должны содержать меры, обеспечивающие контроль:

– выполнения мониторинга, сравнительного анализа и совершенствования среды внутреннего контроля и соответствующей методологии;

– результативности, полноты и эффективности управленческого внутреннего контроля ИС;

– реализации корректирующих действий, вытекающих из оценок системы внутреннего контроля ИС.

5.4.1.3 В процессе обеспечения соответствия ИС внешним требованиям процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– выявления требований законодательства, регулирующих норм и условий договоров;

– анализа и корректировок процедур на предмет соответствия требованиям законодательства, регулирующих норм и условий договоров.

5.4.1.4 В процессе обеспечения корпоративного управления ИС процедуры внутреннего контроля должны содержать меры, обеспечивающие контроль:

– соответствия системы управления ИС общекорпоративному управлению банком и среде контроля;

– информирования руководства банка об эффективности ИС и обеспечении соответствия ИС бизнес-процессам банка и корпоративной стратегии банка;

– использования и распределения ресурсов информационных технологий;

– организации управления ИТ-рисками;

– организации и периодического проведения независимой оценки (внутренней или внешней) соответствия ИС требованиям законодательства и локальных нормативных правовых актов банка, корпоративной политики, стандартов и общепринятых практик, а также эффективности и результативности ИС.

6 Внутренний аудит информационной системы банка

6.1 Планирование внутреннего аудита информационной системы

В процессе планирования внутреннего аудита банка необходимо:

– определить цели и область проведения внутреннего аудита ИС;

– определить ответственных лиц;

– разработать план внутреннего аудита ИС.

6.1.1 Цели и область проведения внутреннего аудита ИС определяются на основе анализа структуры ИС и ее подсистем, их физического расположения и взаимосвязей, а также структуры ролей и распределения ответственности персонала ИС.

6.1.2 План внутреннего аудита ИС должен включать:

– цель внутреннего аудита ИС;

– критерии внутреннего аудита ИС;

– границы внутреннего аудита ИС;

– сроки проведения внутреннего аудита ИС;

– описание процедуры внутреннего аудита ИС;

– распределение ресурсов при проведении внутреннего аудита ИС.

План внутреннего аудита ИС должен определять совокупность оцениваемых ИТ-процессов, ИТ-ресурсов и информационных критериев, последовательность шагов по сбору и анализу информации внутреннего аудита ИС и проведению необходимых тестов.

6.1.3 На этапе планирования определяются наиболее значимые для существующих бизнес-процессов банка информационные критерии: эффективность, полезность, конфиденциальность, целостность, доступность, соответствие и достоверность. Затем идентифицируются ИТ-риски и оценивается общий уровень контроля рассматриваемых бизнес-процессов. При этом принимаются во внимание существующие механизмы управления, последние изменения в ИС банка, зарегистрированные инциденты и результаты предыдущих аудитов ИС. На основе полученной информации осуществляется выбор соответствующих ИТ-процессов и связанных с ними ИТ-ресурсов, служащих объектом исследования в рамках внутреннего аудита ИС.

6.2 Выполнение процедуры внутреннего аудита информационной системы

Выполнение процедуры внутреннего аудита ИС включает следующие этапы:

– идентификация механизмов управления ИТ и документирование (включает в себя получение и первичный анализ информации);

– оценка процессов управления;

– проверка соответствия критериям аудита процессов управления и компонентов ИС;

– детальная проверка процессов управления и компонентов ИС выработка рекомендаций и подготовка отчета;

– контроль за выполнением рекомендаций.

6.2.1 На этапе идентификации механизмов управления ИТ и документирования осуществляется получение, документирование и первичный анализ информации о состоянии ИС, а также идентификация существующих механизмов управления ИТ с учетом выяснения следующих вопросов:

– требования к ИС;

– организационная структура ИС;

– распределение ролей и ответственности;

– политики и процедуры в ИТ;

– требования нормативных правовых актов;

– существующие процессы управления ИТ;

– существующая отчетность в рамках управления ИТ.

Информация о состоянии ИС должна быть пригодна для оценки на ее основе степени соответствия параметров ИС критериям аудита, фактического уровня ИТ-рисков и выработки рекомендаций, направленных на их минимизацию.

6.2.2 На этапе оценки процессов управления производится оценка эффективности существующих процессов управления при выполнении задач управления ИТ, оценивается их целесообразность и пригодность путем сравнения с установленными критериями и стандартами. Аудитору необходимо убедиться в том, что:

– существующие ИТ-процессы документированы;

– ответственность и подотчетность четко определены;

– там, где необходимо, существуют компенсирующие процессы управления ИТ.

6.2.3 Проверка соответствия критериям аудита процессов управления и компонентов ИС осуществляется путем получения прямых и косвенных свидетельств надлежащего выполнения установленных процедур управления за оцениваемый период. На этом этапе проводится оценка соответствия ИС и управления ИТ требованиям нормативных правовых актов и стандартов, а также выполняется ограниченное исследование адекватности результатов процессов управления, определяется уровень детальной проверки и объем дополнительной работы, необходимой для получения подтверждения адекватности ИТ-процессов. Аудитору необходимо получить доказательства пригодности существующих процессов управления для решения задач управления ИТ.

6.2.4 На этапе детальной проверки процессов управления и компонентов ИС, выработки рекомендаций и подготовки отчета выполняется:

а) выявление источников ИТ-рисков, в частности:

1) неготовность ИТ оказывать адекватную поддержку бизнес-процессам банка;

2) высокая длительность и стоимость проектов по созданию и модернизации ИС и ее компонентов;

3) несоответствие фактического уровня ИТ-сервисов и показателей функционирования ИС существующим требованиям;

4) частые сбои и длительное время восстановления работоспособности ИС;

5) неполное использование пользователями возможностей ИС;

6) ошибки при обработке данных в ИС;

7) недостатки в обеспечении полноты контрольных и управленческих процедур, направленных на достижение целей управления ИТ и обеспечения требуемых показателей функционирования ИС;

8) недостатки в системе управления информационной безопасностью, повышающие вероятность нарушения конфиденциальности, целостности и доступности информации в ИС;

9) совокупность недостатков системы управления ИТ в отношении отдельных компонентов ИС, задействованных в поддержке отдельного бизнес-процесса, которые могут привести к реализации рисков банка;

10) неадекватное управление персоналом, что может привести к отсутствию высококвалифицированного персонала, необходимого для выполнения ключевых ИТ-операций;

б) оценка и обоснование ИТ-рисков путем использования аналитических методов и экспертных оценок;

в) ситуационное моделирование, позволяющее оценить адекватность применяемых методов управления и контроля за ИТ для различных условий деятельности, в том числе расширение или изменение масштабов деятельности банка, модернизация или переход на новую ИС, изменение объемов финансирования, отсутствие ключевого персонала ИС;

г) документирование недостатков процессов управления ИТ, угроз и уязвимостей ИС, являющихся следствием этих недостатков, реальных и потенциальных последствий реализации угроз путем причинно-следственного анализа и проведения сравнительного тестирования;

д) подготовка рекомендаций по повышению эффективности внутреннего контроля ИС с целью улучшения состояния ИС и управления ИТ банка;

е) подготовка рекомендаций по совершенствованию методологии оценки ИТ-рисков в условиях динамично изменяющейся среды функционирования ИС;

ж) формирование аудиторского отчета.

6.2.5 На этапе контроля за выполнением рекомендаций осуществляется проверка эффективности принятых мер по исправлению выявленных нарушений в организации внутреннего контроля ИС и выполнения рекомендаций по его совершенствованию.

6.3 Критерии ценности аудиторского отчета

Критериями ценности аудиторского отчета являются:

– достоверность: выводы отчета основаны на фактах, которые могут быть повторно проверены, а так же на изучении достаточного количества информации;

– актуальность: основной акцент в отчете делается на проблемах и рисках, которые уже реализуются или с высокой вероятностью могут быть реализованы в краткосрочной перспективе;

– ясность: информация излагается в структурированном виде – от общих выводов в бизнес-терминах для руководства банка до частных рекомендаций, включающих специфические аспекты, для руководства ИТ;

– полезность (применимость): информация максимально адаптирована для целей формирования планов совершенствования ИС и системы управления ИТ.